Licence Pluridisciplinaire – Mathématiques
Devoir d'algèbre
Corrigé

Exercice 1. Soit $\mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} \mid m, n \in \mathbb{Z}\}$ et $\mathbb{Z}[\sqrt{5}] = \{m + n\sqrt{5} \mid m, n \in \mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[\sqrt{3}]$ et $\mathbb{Z}[\sqrt{5}]$ sont des anneaux commutatifs intègres.

Solution. Soit $x \in \mathbb{R}$. D'après le cours, $\mathbb{Z}[x]$ est un sous-anneau de $\mathbb{R}$: c'est l'image de l'anneau de polynômes $\mathbb{Z}[X]$ à coefficients entiers par la substitution de $x \in \mathbb{R}$ à l'indéterminée X. Reste à vérifier que ces anneaux ont bien la forme indiquée. D'après le théorème du cours,

$$\mathbb{Z}[x] = \left\{ \sum_k a_k x^k \mid (a_k)_{k\in\mathbb{N}} \text{ suite presque nulle d'entiers} \right\}.$$

Comme $x^2 \in \mathbb{Z}$, on en déduit que $\mathbb{Z}[x]$ a bien la forme de l'énoncé pour $x = \sqrt{3}$ et $x = \sqrt{5}$. ■

On pouvait aussi démontrer directement que ce sont des sous-anneaux de $\mathbb{R}$.

2. L'objet de cette question est de montrer que ces deux anneaux ne sont pas isomorphes. Pour cela, on suppose, par l'absurde, qu'il existe un isomorphisme d'anneaux $f : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{5}]$.

2.1. Montrer que $f(n) = n$ pour tout entier n.

Solution. Par définition, $f(1) = 1$ car f est un morphisme d'anneaux (donc envoie unité de l'anneau de départ sur unité de l'anneau d'arrivée). Ensuite $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$. Supposons par récurrence que $f(n) = n$ pour $n \in \mathbb{N}$, alors $f(n + 1) = f(n) + f(1) = n + 1$. Comme $f(-n) = -f(n)$, on en déduit le résultat. ■

2.2. Montrer que $f(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$.

Solution. $3 = f(3) = f(\sqrt{3})^2$, d'où le résultat. ■

2.3. Montrer que $\sqrt{3} \notin \mathbb{Z}[\sqrt{5}]$. Conclure.

Solution. Par l'absurde. Supposons $\sqrt{3} = a + b\sqrt{5}$. Pour obtenir une contradiction : on peut élever au carré, on trouve

$$3 - a^2 - 5b^2 = 2ab\sqrt{5}.$$

Si $ab \neq 0$ alors $\sqrt{5}$ est un rationnel. Montrons que $\sqrt{5}$ n'est pas un rationnel. Si $\sqrt{5} = u/v \in \mathbb{Q}$, avec u, v premiers entre eux, alors $5v^2 = u^2$. Comme 5 est premier, 5 divise u (Gauss). Donc $u = 5u'$. Donc $5v^2 = 25u'^2$ d'où $v^2 = 5u'^2$. Comme 5 est premier, on en déduit que 5 divise v (à nouveau Gauss). Donc 5 divise à la fois u et v : contradiction avec le fait que u et v sont premiers entre eux.

Donc $ab = 0$ ce qui implique $a = b = 0$, contradiction. ■

Exercice 2. L'objet de cet exercice est l'étude d'une classe de nombres premiers. On pourra s'inspirer de la démonstration du cours par l'absurde de l'infinité des nombres premiers.

1. Soit $n \in \mathbb{Z}$ un entier impair. Que peut-on dire de $n \bmod 4$?

Solution. $n \equiv \pm 1 \bmod 4$. ■

2. Soit S l'ensemble des nombres entiers de la forme $4n+1$. Montrer que S est stable par multiplication.

Solution. On peut multiplier les congruences donc si $a, b \equiv 1 \bmod 4$ alors $ab \equiv 1 \cdot 1 \equiv 1 \bmod 4$.

On peut aussi redémontrer ce résultat dans ce cas particulier : si $a = 4n+1$ et $b = 4n'+1$ alors $ab = 16nn' + 4(n+n') + 1 = 4[4nn' + n + n'] + 1$. ■

3. Montrer qu'il existe une infinité de nombres premiers de la forme $4m+3$.

Solution. Notons $\mathcal{P}$ l'ensemble des nombres premiers. D'après les questions précédentes, cet ensemble se décompose en la réunion disjointe

$$\mathcal{P} = \{2\} \cup \mathcal{P}_1 \cup \mathcal{P}_3, \tag{1}$$

où $\mathcal{P}_i = \{p \in \mathcal{P} \mid p \equiv i \bmod 4\}$.

On raisonne par l'absurde. Soit $3 < p_1 = 4n_1 + 3 < \ldots < p_r = 4n_r + 3$ la liste finie des nombres premiers ($\neq 3$) congrus à 3 modulo 4. Considérons le nombre

$$N = 4p_1 \cdots p_r + 3.$$

Ce nombre est impair (donc non divisible par 2) et non divisible par 3. De plus, puisque $N \equiv 3 \bmod 4$, on en déduit que N *n'est divisible par aucun nombre premier* p_i, $i = 1, \ldots, r$.

Supposons (par l'absurde) que N est divisible par un nombre premier de la forme $4n+1$. Si $N = (4n+1)Q$, alors le quotient Q est un entier impair (puisque $4n+1$ et N sont impairs), donc $Q \equiv \pm 1 \bmod 4$. Donc tous les facteurs premiers $q_1, \ldots, q_s$ de Q sont congrus à $\pm 1 \bmod 4$. S'ils sont tous congrus à 1 mod 4, alors par stabilité d'après 2), $Q \equiv 1 \bmod 4$. Donc $N = (4n+1)Q \equiv 1 \bmod 4$ encore d'après 2), ce qui contredit le fait que $N \equiv 3 \bmod 4$. On en déduit donc qu'il existe un facteur $q_i \equiv 3 \bmod 4$ parmi les facteurs premiers de Q. Il existe donc $1 \leq j \leq r$ tel que $q_i = p_j$ divise N, ce qui est absurde.

On en conclut que N n'est divisible ni par 2 ni par un nombre premier de la forme $4n+3$ ni par un nombre premier de la forme $4n+1$. Au vu de (1), on en déduit que N est premier. De plus, $N \equiv 3 \bmod 4$ et $N > p_r$. Contradiction. ■

Exercice 3. Soit $n \geq 2$. Montrer que $x = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ n'est pas un entier.

Solution. L'idée est de regarder *la plus grande puissance de* 2 entre 1 et n (les dénominateurs des fractions). Soit 2^k cette puissance. Remarquons que le seul entier parmi $1, 2, \ldots, n$ que 2^k divise est 2^k : en effet, tout autre entier est nécessairement un multiple de 2^k, donc de la forme $2^k s$ avec $s > 1$. Dans ce cas, $1 \leq 2^k < 2^k \times 2 = 2^{k+1} \leq 2^k s \leq n$, ce qui signifie

que $2^{k+1} \leq n$, ce qui contredit le fait que 2^{k+1} est la plus grande puissance de 2 entre 1 et n.

Nous avons

$$2^{k-1}x = 2^{k-1}\left(\frac{1}{2^k} + \sum_{\substack{1\leq j\leq n\\ j\neq 2^k}} \frac{1}{j}\right) = \frac{1}{2} + \frac{a}{b}$$

où a/b est une fraction irréductible avec b impair (et a pair). Donc

$$2^{k-1}x = \frac{b+2a}{2b},$$

avec $b+2a$ impair et $2b$ pair, d'où l'on déduit $2^{k-1}x \notin \mathbb{N}$. On en conclut que $x \notin \mathbb{N}$. ■